UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

vs. Civil No. 1:23-cv- 1161

86,766.00 USDT seized from OKX account UUID ending 5504 and ID Number '097799 with affiliated deposit address ending 94d8,

Defendant Property.
_____/

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

NOW COMES Plaintiff, United States of America, by and through its attorneys, Mark A. Totten, United States Attorney for the Western District of Michigan, and Daniel T. McGraw, Assistant United States Attorney, and states upon information and belief that:

NATURE OF THE ACTION

1. This is a civil forfeiture action filed pursuant to 18 U.S.C. §§ 981(a)(1)(A), 981(a)(1)(C) and Supplemental Rule G(2) of the Federal Rules of Civil Procedure to forfeit and condemn to the use and benefit of the United States of America 86,766.00 USDT seized from OKX account UUID ending 5504 and ID Number '097799 with affiliated deposit address ending 94d8 (the "Defendant Property").

THE DEFENDANT IN REM

2. The Defendant Property consists of 86,766.00 USDT seized on or about July 2, 2023 from OKX account UUID ending 5504 and ID Number '097799 with affiliated deposit address ending 94d8 by the United States Secret Service (USSS). The Defendant Property is currently in the custody of the USSS.

JURISDICTION AND VENUE

3. This Court has jurisdiction over this proceeding pursuant to 28 U.S.C. §§ 1345 and 1355(b)(1)(A) because this action is being commenced by the United States of America as plaintiff and the acts giving rise to the basis for forfeiture occurred in the Western District of Michigan.

4. Venue is proper before this Court pursuant to 28 U.S.C. § 1395(b), because the Defendant Property is located within the Western District of Michigan.

BASIS FOR FORFEITURE

5. As set forth below, the Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) because it constitutes any property, real or personal, which constitutes or is derived from proceeds traceable to wire fraud, in violation of 18 U.S.C. § 1343, and pursuant to 18 U.S.C. § 981(a)(1)(A), 981(a)(1)(C), because it is property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956, or property that constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1956, money laundering.

FACTS SUPPORTING FORFEITURE

Background on "Pig Butchering" Schemes

6. Criminal organizations engage in a variety of fraud schemes to convince an unsuspecting victim to send co-conspirators money. One scheme involves "pig butchering," where online co-conspirators utilize social media platforms and dating websites in search of fraud victims. The scheme involves a suspect creating a fake social media or dating profile that is then used to reach out to potential fraud victims through social media, dating sites, and even through random text messaging.

7. The "pig butchering" scheme typically begins with the suspect initiating cordial conversation with a victim, with the goal of becoming the victim's "friend" or romantic "lover." The suspect often creates reasons to continue a conversation, which then leads to multiple follow up phone calls or additional communications. The suspect and victim slowly develop a relationship so that the suspect can insert themself into the victim's daily life. While slowly building trust with the victim, the suspect will start to introduce the idea of making business investments using cryptocurrency. The suspect will employ persuasion rather than requesting money outright because the suspect is aware that often, the targeted victim is savvy and will know that requests for money from a stranger is one sign of a potential scam or fraud scheme.

8. Gradually, the victim is drawn into what appears to be benign conversation about cryptocurrency investments and potential earnings but is really the groundwork for manipulation to make an "investment." Ultimately, once trust is

gained, the suspect will convince the victim to invest in cryptocurrency and refers the victim to a bogus website or application that looks authentic but is controlled by the suspect or his criminal co-conspirators. The victim is then encouraged to invest small amounts in the beginning, and the suspect will ensure to post a modest gain on that initial small investment. The suspect might even allow the victim to withdraw money once or twice to convince the victim that the process and investments are legitimate. The suspect will then persuade the victim to invest larger amounts through the fake platform, sometimes for hundreds of thousands of dollars. Once the larger amount of money is transferred, the suspect disappears, taking all the money, which results in significant financial loss for the victim.

9. Often, criminal organizations will commit "money laundering," as defined by 18 U.S.C. § 1956, to disguise the illicit nature of funds, by either introducing it into legitimate commerce and finance, thereby making it "clean," or by engaging in multiple subsequent transactions to disguise the true origin of the funds. This process commonly occurs in three steps: placement, layering, and integration. Typically, the placement phase takes place when proceeds from illicit sources are placed in a financial institution or business entity. Layering takes place when these funds are then used in seemingly legitimate commerce transactions, which makes the tracing of the funds more difficult and further removed from the originating criminal activity. Finally, the integration phase is when these funds are used to promote the unlawful activity or for the personal benefit of the individuals involved.

Background on Cryptocurrency and Cryptocurrency Exchanges

10. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency include Bitcoin, Litcoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries.

11. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction. The blockchain can be updated multiple times per hour and record every virtual currency address that ever received that virtual currency. It also maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

12. Although cryptocurrencies such as Bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes,

such as money laundering, and is often used for means of payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to trace transactions.

13. Virtual currency addresses are the virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of alphanumeric characters.

14. Each virtual currency address is controlled using a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

15. A virtual currency wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet.

16. Bitcoin ("BTC") is a type of cryptocurrency. Payments or transfers of value made with Bitcoin are recorded in the Bitcoin blockchain, and thus are not maintained by any single administrator or entity. Individuals can acquire Bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), Bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by "mining." Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even

though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And while it is not completely anonymous, Bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

17. USDC is another well-known and popular cryptocurrency "stablecoin" pegged to the U.S. dollar and according to the company's website, "can always be exchanged 1:1 for cash." USDC can also be held on more than one blockchain, including the Ethereum blockchain. Similar to another cryptocurrency called USDT, which is issued by Tether, USDC is popular with cryptocurrency scams due to the fact that it retains its value in relation to the dollar and its value does not fluctuate to the extent of other digital currencies.

18. USDT is a blockchain-based cryptocurrency whose tokens in circulation are backed by an equivalent amount of U.S. dollars, making it what is known as a "Stablecoin." USDT is issued by Tether Ltd., a company headquartered in Hong Kong. Tether is a subsidiary of Bitfinex, a cryptocurrency exchange registered in the British Virgin Islands. USDT is hosted on the Ethereum and Bitcoin blockchains, among others. Ethereum ("ETH") is a cryptocurrency that is open source, public, has a

blockchain, and is distributed on a platform that uses "smart contract" technology. The public ledger is the digital trail of the Ethereum blockchain, which allows anyone to track the movement of ETH.

19. Smart contracts allow developers to create markets, store registries of debts, and move funds in accordance with the instructions provided without any type of middleman or counterparty controlling a desired or politically motivated outcome, all while using the Ethereum blockchain protocol to maintain transparency. Smart contract technology is one of Ethereum's distinguishing characteristics and an important tool for companies or individuals executing trades on the Ethereum blockchain. When engaged, smart contracts automatically execute according to the terms of the contract written into lines of code. A transaction contemplated by a smart contract occurs on the Ethereum blockchain and is both trackable and irreversible.

20. Like other virtual currencies, USDT is sent to and received from USDT "addresses." A USDT address is somewhat analogous to a bank account number and is represented as a 26-to 35-character-long case-sensitive string of letters and numbers. Users can operate multiple USDT addresses at any given time, with the possibility of using a unique USDT address for every transaction. Although the identity of a USDT address owner is generally anonymous (unless the owner opts to make the information publicly available), analysis of the blockchain can often be used to identify the owner of a particular USDT address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity.

21. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). Individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured, in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

22. Virtual Currency "exchangers" and "exchanges" are individuals or companies that exchange Bitcoin for other currencies and cryptocurrencies, including U.S. dollars and tether. According to Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses ("MSBs"). Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). Registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10%, in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%

Pig Butchering Victim from Grandville, Michigan Reports Fraud

23. On January 28, 2023, fraud victim Z.L. contacted USSS Chicago Field Office and reported being the victim of an online romance/investment fraud scheme. Z.L., a resident of Grandville, Michigan, within the Western District of Michigan, stated that on or about December 8, 2022, Z.L. received an unsolicited text message from a person purporting to be "Guo Jintong Teresa" (Jintong_0206) via an application identified as WeChat. Z.L. engaged in online conversations with Guo Jintong Teresa on WeChat and Line. During subsequent conversations, Z.L. received information concerning an investment opportunity from Guo Jintong Teresa. Z.L. continued the online conversations and Guo Jintong Teresa provided a link to penzolead.com. Guo Jintong Teresa indicated the website conducted short-term forex trading of Bitcoin, which was investing based on the rise and fall of Bitcoin in a short period of time.

24. On December 14, 2022, Z.L. made an initial deposit of $1,000 via his Bank of America ("BOA") debit card to the cryptocurrency account/address associated with penzolead.com. The following day, Z.L. was provided a return of $190 on this initial investment. This return on the initial investment added legitimacy to the investment opportunity.

25. Following the success of the initial investment, Z.L. invested additional funds. An analysis of Z.L's BOA account ending 4082 ("**BOA 4082**") showed the following transactions between BOA 4082 and Z.L's Cyrpto.com account, User ID ending 2594 ("**Crypto 2594**").

Date Received	**Amount**	**Beneficiary**	**Notes**
12/22/22	$19,000.00	MCB FORIS / Crypto.com	BOA wire on 12/19/22
12/30/22	$20,000.00	MCB FORIS / Crypto.com	BOA wire on 12/30/22
1/6/23	$47,000.00	MCB FORIS / Crypto.com	BOA wire 01/05/23
1/10/23	$15,000.00		Returned to Z.L.
1/18/23	$50,000.00	MCB FORIS / Crypto.com	BOA wire on 01/18/23
1/20/23	$50,000.00	MCB FORIS / Crypto.com	BOA wire on 01/20/23
Total	$186,000 -$15,000 $171,000	Sent Received Back Total Loss	

26. On January 10, 2023, Z.L. received a $15,000 disbursement in **Crypto 2594**. The funds were then sent to **BOA 4082** on January 11, 2023. This deposit again gave credibility and legitimacy to the investment opportunity, and enticed Z.L. to further invest. In total, between December 19, 2022 and January 20, 2023, Z.L. wired $186,000, less the $15,000 Z.L. received back, for a total "investment" (or loss) amount of $171,000.

27. On January 25, 2023, Z.L. received an email from Crypto.com requesting Z.L. review his transaction history. The email stated that Crypto.com regularly investigates scams, and the wallet addresses associated with them. In the most recent review, Crypto.com found some of Z.L.'s crypto transactions were linked to one or more wallet addresses associated with a scam. Crypto.com strongly suggested Z.L. review transactions between October 2022 and January 2023. Z.L. then conducted an open-source search for Penzo Limited and discovered an online alert issued on

December 29, 2022 by the California Department of Financial Protection and Innovation ("DFPI") concerning cryptocurrency broker Penzo Limited. The DFPI stated the agency received a complaint from a California resident indicating the victim was contacted via Facebook promising great returns in cryptocurrency investing. The victim wired funds to Coinbase to purchase cryptocurrency, then sent that to the MetaTrader5 platform through a mobile device. The scammer showed a demo example where a $100,000 investment could earn profits of $11,000. The scammer showed the victim pictures of their lavish lifestyle and said they could help them achieve success. The scammer then walked the victim through a step-by-step process, transferring their money into the scammer's account on the platform, then sending screenshots showing they had earned $200,000. The scammer then asked the victim if they wanted to transfer more money. At that point the victim became concerned and asked for their money back. The scammer told them that they had lost all of their money and it was their fault for making bad trades. The DFPI identified the company operating the website as https://penzolead.com.

28. Z.L. then attempted to withdraw the funds, due to concerns from the alert; however, Z.L.'s withdrawal attempt was denied through the penzolead.com website. Z.L. contacted customer listed on the website, and engaged in a chat with an unknown representative. The unknown representative advised Z.L. was required to pay taxes prior to the withdrawal, and provided an additional Bitcoin address for Z.L. to pay taxes. Z.L. was then confident that it was a fraud scam, and declined to make further payments.

29. https://penzolead.com is no longer accessible as a website.

Crypto.com/Foris Dax, Inc./Foris Inc., User ID ending 2594

30. As shown above, Z.L. sent a total of $186,000.00 from **BOA 4082** to **Crypto 2594**, over which Z.L. has full ownership. After **Crypto 2594** received the USD deposits, the funds were then converted into cryptocurrency. Specifically, the funds were swapped from US dollars to USDC, which is a type of cryptocurrency referred to as a stablecoin entailing a 1:1 ratio with the US dollar in value (as described above). Review of **BOA 4082** showed that Z.L. made five deposits from **BOA 4082** to **Crypto 2594** totaling the $186,000.00. The current loss is $171,000.00, due to the return of $15,000.00 to Z.L.

31. Records from Crypto.com for **Crypto 2594** show that Z.L.'s funds were used to purchase stablecoin, USDC. Once the USDC was purchased through the Crypto.com/Foris Inc, cryptocurrency platform, they were then sent to other cryptocurrency platforms that were not in the name of, or under the control, of Z.L. Multiple transactions like this are commonly done by individuals engaging in this type of fraud, and make it easier for these subjects to launder the fraudulent funds and make it more difficult for law enforcement to trace.

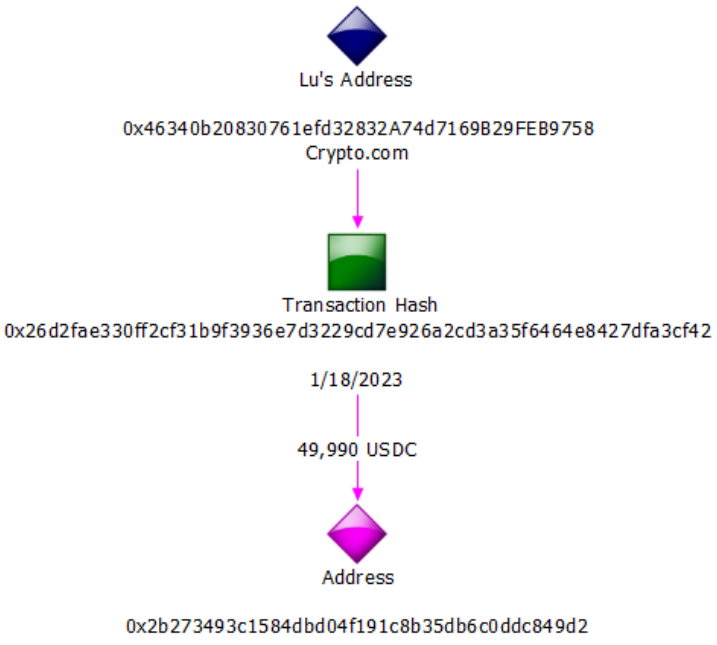
OKX Account UUID ending 5504 (OKX 5504)

32. OKX is one of the largest cryptocurrency exchanges in the world, in terms of daily trading volume of cryptocurrencies. It was founded in 2017 and is registered in the Seychelles. OKX is a full-service cryptocurrency exchanger and offers service to account holders that involve facilitating the purchase, sale and

transfer of a variety of digital currencies. The target identifier for the Defendant Property enabled OKX to uniquely identify an account.

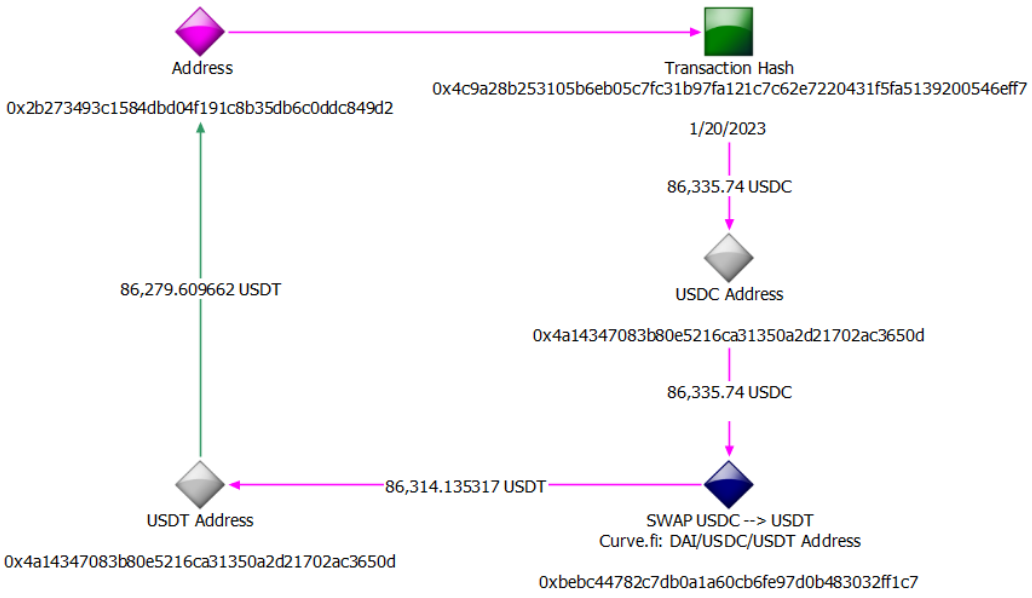
33. As described above, once the funds from Z.L. left **Crypto 2594**, the funds were no longer under the control of Z.L. The funds were under the control of unidentified subjects, who then used the funds for additional cryptocurrency purchases. Again, such transactions disguise the true nature of the stolen funds, and make it more difficult for law enforcement to detect and potentially seize those funds to return to victims.

34. As part of this investigation, a USSS Investigative Analyst (IA) traced the multiple cryptocurrency transactions. Using blockchain analysis, USSS IA conducted an analysis of the **Crypto 2594** account and traced the funds that were sent from **Crypto 2594** to an unknown USDC address: 0x2b273493c1584dbd04f191c8b35db6c0ddc849d2 ("**USDC/T 49d2**"). A review of records showed the following transactions: (1) January 18, 2023: $50,000 sent from **BOA 4082** to **Crypto 2594**; and (2) January 18, 2023: $50,000 exchanged for 49,990 USDC in **Crypto 2594** and sent to **USDC/T 49d2**. *See* Figure A:

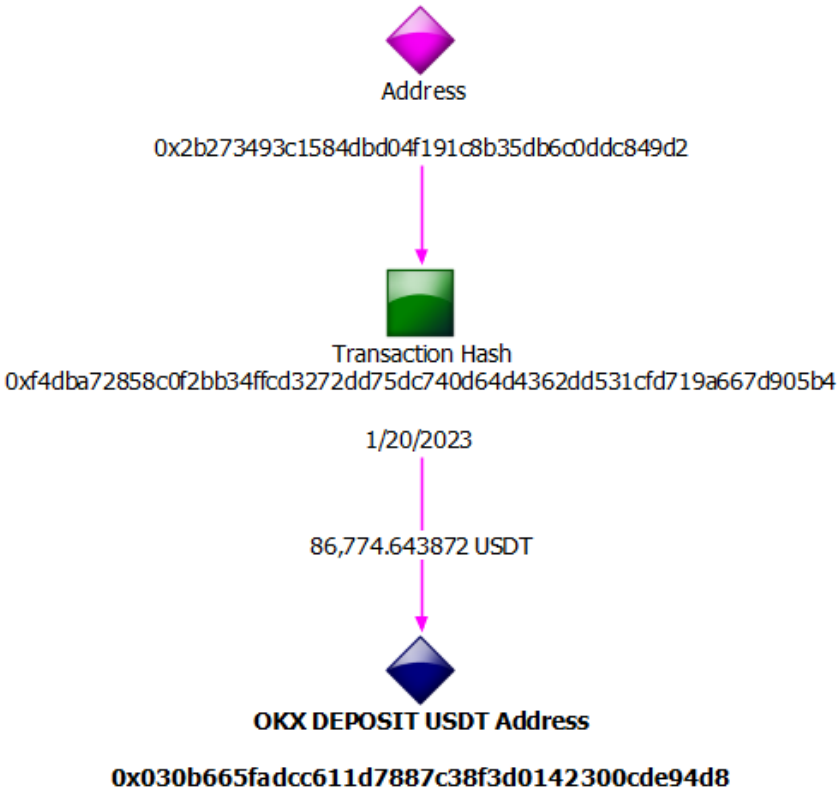


35. According to information received from the Federal Bureau of Investigation ("FBI"), a "pig butchering" victim from Kentucky filed a report indicating they were scammed into sending funds to a cryptocurrency wallet. The Kentucky victim requested a withdrawal of the funds, but was denied, while the unknown suspect(s) requested an additional $30,000 be deposited to the same unknown USDC address **USDC/T 49d2** where Z.L. funds were transferred.

36. Blockchain analysis on **USDC/T 49d2** shows that on January 20, 2023, a cryptocurrency "swap" took place in a transaction of swapping USDC for USDT. **USDC/T 49d2** sent 86,335.74 USDC to address **0x4a14347083b80e5216ca31350a2d21702ac3650d** ("**USDC/T 650d**"). In order to complete the "swap." **USDC/T 650d** sent the 86,335.74 USDC to swap address 0xbebc44782c7db0a1a60cb6fe97d0b483032ff1c7 ("**SWAP f1c7**"). **SWAP f1c7** completed the "swap" and sent 86,314.135317 **USDT** back to **USDC/T 650d**. **USDC/T 650d** then sent 86,279.609662 USDT to the initial address, **USDC/T 49d2**. *See* Figure B:



37. On January 20, 2023, after confirming the deposit of 86,279.609662 USDT into **USDC/T 49d2** through blockchain analysis, **USDC/T 49d2** sent 86,774.643872 USDT to OKX Address **0x030b665fadcc611d7887c38f3d0142300cde94d8** ("**OKX 94d8**"). *See* Figure C:



38. A USSS financial analysis of **OKX 94d8** confirmed the deposit of 86,774.643872 USDT on January 21, 2023. The funds contained in **OKX 94d8** were the proceeds of a "pig butchering" wire fraud scheme. A criminal organization fraudulently persuaded Z.L. under false pretenses to transfer funds from **BOA 4082**, and through subsequent transfers to conceal the origin of the funds, those funds were ultimately deposited into **OKX 94d8**.

39. On or about July 2, 2023, USSS executed a federal seizure warrant for the Defendant Property, which is 86,766.00 USDT seized from OKX account UUID ending 5504 and ID Number‘097799 with affiliated deposit address end 94d8 as property, real or personal, which constitutes or is derived from proceeds traceable to wire fraud, in violation of 18 U.S.C. § 1343, and as property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956, or property that constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1956, money laundering.

CLAIM I
(Forfeiture of Proceeds Traceable to Wire Fraud)

40. Plaintiff hereby incorporates by reference the allegations set forth in paragraphs numbered 1 through 39, as referenced above.

41. The Defendant Property is forfeitable to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) because it constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1343.

CLAIM II
(Forfeiture of Property Involved in or Proceeds of Money Laundering)

42. Plaintiff hereby incorporates by reference the allegations set forth in paragraphs numbered 1 through 39, as referenced above.

43. The Defendant Property is forfeitable to the United States pursuant to pursuant to 18 U.S.C. § 981(a)(1)(A), 981(a)(1)(C), because it is property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956, or property that constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1956.

RELIEF

Wherefore, the United States prays that the usual process for forfeiture issue against the Defendant Property; that due notice be given to all interested parties to appear and show cause why forfeiture to the United States of America should not be decreed; and that the Defendant Property be condemned and forfeited to the United States of America and be delivered into the custody of the United States Secret Service for disposition according to law; and for such other relief as this Court may deem just and proper.

MARK A. TOTTEN
United States Attorney

Dated: November 1,2023

DANIEL T. McGRAW
Assistant United States Attorney
P.O. Box 208
Grand Rapids, MI 49501-0208
(616) 456-2404

VERIFICATION

I am a Special Agent with the United States Secret Service and I am the lead investigator of the fraud scheme described herein.

I have read the contents of the foregoing Verified Complaint for Forfeiture *In Rem* and the statements contained therein are true to the best of my knowledge and belief.

I declare under penalty of perjury that the foregoing is true and correct.

Dated: November 1, 2023

DANIEL KESLING
Special Agent
United States Secret Service